



Chapter 1

Health and Wellness; Internal Services; IWK Health Centre; and Nova Scotia Health Authority: Management and Oversight of Health Sector Information Technology

Overall Conclusions

- The Department of Health and Wellness does not provide effective leadership and direction on information technology (IT) in the health sector
- The four government organizations responsible for IT in the health sector (Department of Health and Wellness; Department of Internal Services; IWK Health Centre; Nova Scotia Health Authority)
 - have not formalized roles and accountabilities
 - do not adequately manage IT risks

Accountability for Information Technology in the Health Sector

The four entities have not finalized key agreements for centralized health sector IT services

- A roles and accountabilities exercise started in 2017 is ongoing as of fall 2018
- An Executive Committee proposed to provide strategic oversight has not met

The health sector does not adequately monitor IT service levels

- Health sector does not ensure that required service levels are met by providers
- Contracts, with one dating back to 1996, have not been reviewed or updated

Managing Information Technology Risks in the Health Sector

The four entities do not have adequate risk management frameworks

- Health and Wellness and Internal Services do not have risk management frameworks
- IWK and Health Authority frameworks have risk identification and mitigation weaknesses

Internal Services and the Health Authority do not have policies requiring IT controls to be monitored

The four entities do not ensure that collective risk to the health sector is adequately managed



Recommendations at a Glance

Recommendation 1.1

The Department of Health and Wellness, Department of Internal Services, IWK Health Centre, and Nova Scotia Health Authority should finalize agreements related to information technology services in the health sector, including the roles and accountabilities of each entity.

Recommendation 1.2

The Department of Health and Wellness, Department of Internal Services, IWK Health Centre, and Nova Scotia Health Authority should evaluate the transition to centralized information technology services, and identify lessons learned which can be applied to future collaborative health sector initiatives.

Recommendation 1.3

The Department of Health and Wellness, IWK Health Centre, and Nova Scotia Health Authority should develop and implement policies for the management of IT service levels, including periodic review of agreements and monitoring of service levels.

Recommendation 1.4

The Department of Health and Wellness, Department of Internal Services, IWK Health Centre, and Nova Scotia Health Authority should develop and implement comprehensive risk management frameworks which include risk management policies, risk registers, a defined risk tolerance, and risk mitigation strategies.

Recommendation 1.5

The Department of Internal Services and Nova Scotia Health Authority should ensure policies are in place to require that IT controls are monitored, results are reported, and deficiencies are managed.

Recommendation 1.6

The Department of Health and Wellness, Department of Internal Services, IWK Health Centre, and Nova Scotia Health Authority should establish a process to assess if IT risks are collectively identified, assessed, and mitigated.

1 Health and Wellness; Internal Services; IWK Health Centre; and Nova Scotia Health Authority: Management and Oversight of Health Sector Information Technology

Accountability for Health Sector IT

- 1.1 Information technology (IT) provides clinicians and support staff in the health sector with the tools and information needed to effectively and efficiently manage and provide care to Nova Scotians. A broad range of information systems are used in healthcare facilities; registration and scheduling systems, lab diagnostic systems, electronic health records, and other clinical applications allow health care facilities to organize patient flow, analyze and store lab results, and keep detailed medical histories.
- 1.2 Ensuring effective and efficient health care requires that information technology systems and personal health information remain secure and available. Failure to do so can have significant impacts. Potential consequences include unauthorized disclosure of personal health information, increased wait times for services, increased costs to the health care system, and overall negative impacts on the health and well-being of Nova Scotians.



Department of Health and Wellness is not effectively leading IT in the health sector

- 1.3 The Department of Health and Wellness has not provided the level of leadership and direction required to effectively transition the health sector to centralized information technology services. There are no signed agreements for the delivery of IT services in the health sector, roles and accountabilities are not clear, key service levels are not monitored and reported, and IT risk management is inadequate. These issues leave the Province with a greater risk of significant IT-related deficiencies not being identified or adequately managed. We discuss each issue in more detail throughout this chapter.
- 1.4 The provincial health sector consists of the Department of Health and Wellness, the IWK Health Centre (IWK) and the Nova Scotia Health Authority. Subsequent to the introduction of the Shared Services Act, the mandate of the Department of Internal Services expanded in 2016 to include the network and systems supporting the applications used and managed by the health sector. These four organizations can only meet the IT needs of the health sector if they work together with effective leadership from Health and Wellness.



- 1.5 Health and Wellness is accountable for the performance of the health system and needs to ensure that the Health Authority and the IWK fulfill their responsibilities. Internal Services is a service provider to the health sector, therefore Health and Wellness is also ultimately responsible for both the overall operation of the health system and to ensure the services required from Internal Services are clearly established and performance is monitored.
- 1.6 The recommendations throughout this chapter are directed at the entities responsible to act; however, Health and Wellness must provide more leadership and direction to ensure IT services and IT risks in the health sector are appropriately governed and managed. The completion of the following recommendations will support enhanced leadership.

 Government entities do not have signed agreements for centralized health sector IT services

- 1.7 There are no signed agreements for IT services provided by Internal Services or the Health Authority to support the entities in the health sector. While the four entities work together to ensure IT aligns with the needs of the health sector, agreements are critical when obtaining IT services from another organization to ensure that services required are received. Agreements should define roles and accountabilities, what services are contracted, and the level to which they are to be provided. Not having agreements in place increases the risk of misunderstandings regarding expectations and gaps in services, and limits the ability to hold providers accountable.
- 1.8 A draft agreement exists between the Health Authority and the IWK for the management of the IWK's clinical applications. Health Authority and IWK management indicated this draft agreement was verbally agreed to, although not formalized. There is however no agreement between the Health Authority and Health and Wellness for IT services provided to support the Department's clinical applications.
- 1.9 Three draft agreements exist between Internal Services and the health sector for the delivery of central IT services. Questions surrounding roles and accountabilities have resulted in these contracts remaining unsigned and in ongoing negotiations.

 Health sector has not formally agreed upon roles and accountabilities, including clinical applications

- 1.10 A roles and accountabilities exercise involving all four organizations was initiated in fall 2017; the results are yet to be determined as of fall 2018. One issue in clarifying roles and accountabilities and finalizing the agreements is obtaining consensus on responsibilities for clinical applications.



- 1.11 The health sector has responsibility for clinical applications, and as part of the transition to centralized IT services there was significant discussion around the Health Authority taking responsibility for all clinical applications. No formal decision was made on the roles and accountabilities for clinical applications.
- 1.12 Currently, Health and Wellness manages several significant health applications such as Panorama, Drug Information System, and Personal Health Records. Health and Wellness management defines these as digital health applications supporting provincial health programs that extend beyond the responsibility of the Health Authority. However, Health Authority management considers these applications clinical and feel they should be within their mandate.
- 1.13 Documents from 2014 prepared by an internal working group which included Health and Wellness, and a consultant's report outlining a model for the management of clinical applications, clearly classify the applications as clinical. In fall 2015, a decision request was prepared to approve these documents which include the definition of a clinical application and listings classifying clinical and non-clinical applications.
- 1.14 This is an example of the issues that occur when leadership and direction are not effective in resolving key issues. A decision which was considered at length remains an ongoing issue, more than three years after the creation of the Health Authority. The health sector did not formalize and agree upon roles and accountabilities before the implementation of a significant transition and change in operations. There is an increased risk that roles and accountabilities are not fulfilled as required to best support the health sector due to lack of clarity and agreement.



Proposed Executive Committee is not meeting to provide strategic oversight

- 1.15 The draft agreements between the entities propose three new committees – an Executive, a Health Information Management and Technology Governance, and a Management Committee. While the governance and management committees are meeting, the Executive Committee is not.
- 1.16 The purpose of the Executive Committee is to ensure IT services meet the needs of the health sector. This Committee is critical, as the proposed responsibilities include providing strategic oversight, monitoring the delivery of services, and resolving disputes between the organizations. The issues addressed in this chapter indicate there is a need for this Committee, or alternative governance structure, to be formalized to provide this high-level oversight.

Recommendation 1.1

The Department of Health and Wellness, Department of Internal Services, IWK Health Centre, and Nova Scotia Health Authority should finalize agreements related to information technology services in the health sector, including the roles and accountabilities of each entity.

Joint Response: The Departments, IWK and NSHA agree with this recommendation and are in the process of signing the referenced agreements. At the September 13, 2017 Governance meeting, and under the commitment to continuous improvement, the four organizations identified the need to define clearer roles and accountabilities and began a RACI (responsible, accountable, consulted and informed) exercise as a foundation to building stronger health IT governance. This work continues and is a priority. The RACI will complement the existing agreements and will align with the COBIT framework.



Health sector should apply lessons learned from the transition to future large initiatives

- 1.17 While the health sector has not finalized roles and accountabilities for centralized IT services, the organizations are currently planning another significant Health and Wellness IT strategic initiative.
- 1.18 “One Person, One Record” (OPOR) is a partnership of the four organizations and will replace hundreds of aging clinical applications with a single centralized health information system for the Health Authority and the IWK. The IT strategies of the Health Authority and the IWK are in line with this major initiative. Internal Service’s IT strategic plan to deliver effective IT services supports it as well.
- 1.19 Clearly-defined roles and accountabilities are key to the effective implementation of any large strategic initiative and will be very important in the successful introduction of a centralized health information system in Nova Scotia. This project will have a direct impact on the delivery of health services, and therefore the health and well-being of Nova Scotians. The entities must ensure they identify the key issues which impacted the collaborative relationship throughout the transition to centralized information technology services and ensure they do not continue to impact future initiatives.

Recommendation 1.2

The Department of Health and Wellness, Department of Internal Services, IWK Health Centre, and Nova Scotia Health Authority should evaluate the transition to centralized information technology services, and identify lessons learned which can be applied to future collaborative health sector initiatives.



Joint Response: The Departments, IWK and NSHA agree with this recommendation and will document lessons learned in a summary document. This work has begun and will inform current and future collaborative health sector initiatives. The RACI referenced in 1.1 will clarify roles and accountabilities.

➤ Health sector is not monitoring service levels

- 1.20 The health sector is not ensuring service providers deliver IT services at the required levels. As an example, a service level requirement may define the acceptable amount of time a system can be down before the service provider is required to respond. A lack of, or improper response by a service provider, can increase the amount of time a system is not effectively supporting the delivery of health care and could directly impact patients.
- 1.21 It is the responsibility of Health and Wellness, the Health Authority and the IWK to ensure their IT service providers do what they are contractually required to do. This includes obtaining and reviewing reports on key performance metrics to ensure agreed-upon levels are met.
- 1.22 Internal Services does not report service levels to the health sector for the delivery of IT services. The draft master agreement between the four organizations requires Internal Services to submit quarterly and annual reports to the Executive Committee; however, as noted, this Committee is not meeting and these reports are not submitted elsewhere to the health sector organizations.
- 1.23 The Health Authority is reporting on service levels to the IWK for its management of clinical applications. The Health Authority is not reporting on service levels to Health and Wellness, as there is no agreement with the Department, as previously addressed in this chapter.
- 1.24 The Health Authority does not receive service level reports for clinical applications from various external vendors. In addition to effectively monitoring ongoing operations, this is a concern for overall contract management. Health Authority management stated that review of IT contracts is based on need and risk; however, the vendor contracts relating to two of the Health Authority's significant clinical applications were not reviewed or updated upon the creation of the Health Authority. These contracts, dating as far back as 1996, may no longer reflect the service levels required.

Recommendation 1.3

The Department of Health and Wellness, IWK Health Centre, and Nova Scotia Health Authority should develop and implement policies for the management of IT service levels, including periodic review of agreements and monitoring of service levels.



Joint Response: DHW, IWK and NSHA agree with this recommendation and DHW will lead the development of a joint policy on the management of IT service levels within the health sector. The key clinical applications that underpin the current health IT system have undergone a preliminary assessment to identify those agreements that will be subsumed by OPOR (for example the 1996 agreement referenced in the audit), those that will no longer be required when OPOR is in place and those that will continue separate from OPOR. The policy will identify requirements for periodic review of service agreements and the management and monitoring of service levels. This work has already commenced, and the policy will align with the COBIT framework.

IT Risk Management



The four organizations do not have adequate risk management frameworks

1.25 The four organizations have weaknesses in IT risk management, varying from a complete lack of a risk management framework to significant gaps in the requirements for a robust framework. An effective enterprise risk management framework requires an entity to identify, assess, respond to, and appropriately control risks which may have an undesired impact on the organization.

1.26 We assessed whether each entity had in place the key components of an established risk management framework, including a:

- high-level risk management policy;
- risk register which clearly states risks identified;
- defined risk tolerance; and,
- risk mitigation strategies to reduce risk to the acceptable level.

IT Risk Management Framework	DHW	ISD	IWK	NSHA
Risk management policy	No	No	Yes	Yes
Risk register	No	Partial	Partial	Partial
Defined risk tolerance	No	No	Yes	No
Risk mitigation strategies	No	Partial	No	Partial

1.27 The Departments of Health and Wellness and Internal Services do not have enterprise risk management frameworks in place; however, Internal Services developed a risk register to identify and mitigate cybersecurity risks.

1.28 The IWK implemented an enterprise risk management framework to identify and assess risks to the organization. Although it recognized the risks to the entity, it did not establish mitigation strategies to address and control them.



- 1.29 The Health Authority also implemented an enterprise risk management framework; however, management at the Health Authority has not defined and communicated the level of risk it is willing to accept. By not defining a risk tolerance, the Health Authority may not properly address a risk with a potential impact greater than it is willing to accept, or may over allocate resources to a risk that would not significantly impact the entity or its stakeholders.
- 1.30 We also identified some areas where the risk registers maintained by the Health Authority and the IWK failed to consider some IT security risks that could impact their organizations. Examples include the risk of unauthorized access to personal health information by employees or vendors, and the risks associated with outsourcing for and providing information technology services. These are key risks to consider in protecting the security of the Province's information technology and may indicate the Health Authority and the IWK require a more thorough assessment of IT risks.

Recommendation 1.4

The Department of Health and Wellness, Department of Internal Services, IWK Health Centre, and Nova Scotia Health Authority should develop and implement comprehensive risk management frameworks which include risk management policies, risk registers, a defined risk tolerance, and risk mitigation strategies.

Joint Response: The Departments, IWK and NSHA agree with this recommendation as it applies to health IT service delivery. Risk management practices including risk registers, risk tolerance assessment and risk mitigation strategies will align with the COBIT framework and will include continuous processes that support new initiatives and ongoing operations.



Internal Services and Health Authority do not have policies for monitoring control effectiveness

- 1.31 We enquired with senior management at Internal Services and the Health Authority, as the two entities provide IT services, and determined that neither has policies requiring IT controls to be monitored or deficiencies to be addressed in a timely manner and reported to management. The lack of policies does not support an adequate level of direction and oversight.
- 1.32 The risk of IT controls not being adequately monitored in the health sector is increased without direction and oversight from those charged with governance. IT controls must be monitored, to ensure the protection of health information and systems supporting the delivery of health care services.



Recommendation 1.5

The Department of Internal Services and Nova Scotia Health Authority should ensure policies are in place to require that IT controls are monitored, results are reported, and deficiencies are managed.

Joint Response: The Department of Internal Services and the NSHA agree with this recommendation and will be developing a joint policy. The policy will identify the agreed upon IT controls that will be monitored and reported, to be approved and overseen by DHW.

➡ The four organizations are not collectively managing health sector IT risks

- 1.33 IT risks that could impact the entire health sector are not effectively managed. The failure of one organization to effectively secure its systems against unauthorized access or cybersecurity attacks could have a negative impact on all organizations within the health sector.
- 1.34 The draft service level agreement between Internal Services and the health sector allows Internal Services to hire an independent organization to assess the IT controls at the IWK and the Health Authority. However, Health and Wellness, the IWK, and the Health Authority do not have the authority to obtain an independent assessment of Internal Service's IT controls. Risks related to information technology can impact both service providers and receivers, therefore these organizations may be exposed to control deficiencies and risks from the Department of Internal Services, without the ability to assess and mitigate those risks.
- 1.35 The draft agreement for management of the IWK's clinical applications by the Health Authority does not include an independent assessment to verify the effectiveness of the IT controls in place to protect the IWK's information. Health and Wellness does not have an agreement with the Health Authority and does not require an independent assurance report on IT controls.
- 1.36 The IT security of the health sector is dependent on several organizations effectively managing IT risks. Each organization needs to ensure the others have effectively managed risks and implemented the necessary IT controls through collaboration, self-reporting, or independent assurance reports.

Recommendation 1.6

The Department of Health and Wellness, Department of Internal Services, IWK Health Centre, and Nova Scotia Health Authority should establish a process to assess if IT risks are collectively identified, assessed, and mitigated.

Joint Response: The Departments, IWK and NSHA agree with this recommendation and the process will be put in place as part of the response to recommendation 1.4. The framework will provide the foundation to establish a process to assess IT risks collectively, ensuring they are identified, assessed and mitigated.



Additional Comments from Health and Wellness; Internal Services; IWK Health Centre; and Nova Scotia Health Authority

Providing high quality health care is dependent in part on modernized and integrated health information systems. Nova Scotia's goal is the creation of a single integrated health record for every Nova Scotian. One Person One Record (OPOR) will support and enable clinical transformation and improved health care delivery in Nova Scotia, creating a high functioning, data driven, agile, digital system. This goal guides our work in health sector IT, including steps to have greater coordination and integration of existing systems as we work toward OPOR.

While this work was not in scope for the OAG audit, it informs our response to the findings in this audit. The recommendations from this audit will be aligned with the OPOR Governance structure, clarifying accountability for IT in the health sector. Recommendations 1.2 through to 1.6, will be completed through the lens of OPOR and the lessons learned from transition. Work has been underway:

- In October, the Health Information Management/Information Technology Governance Committee updated their Terms of Reference to support the operational and strategic work underway in health sector IT. The Committee adopted COBIT as the Business Framework for the Governance and Management of Health Sector IT. COBIT is a generally accepted source of best practices, enabling IT to be governed and managed in a holistic manner, by maintaining a balance between realizing benefits and optimizing risk level and resource use. DHW will lead the development of a plan to implement COBIT. The plan will outline the work required and the timelines for completing the supporting policies, templates and procedures.*
- In November, the Health System IMIT Executive Sponsors Committee approved changes to the OPOR Governance structure to confirm clear accountability and oversight exists for all health sector IT. Updated Terms of Reference have been approved for both the Governance Committee and the Executive Committee.*
- Work has begun to obtain an independent assessment of our current state and to provide guidance on the development of a COBIT implementation roadmap and plan for any improvements identified.*
- To summarize, the Departments, IWK and NSHA intend to implement all recommendations related to the Management and Oversight of Health Sector IT.*



Reasonable Assurance Engagement Description and Conclusions

In fall 2018, we completed an independent assurance report of the management and oversight of health sector IT of the Department of Health and Wellness; Department of Internal Services, IWK Health Centre and Nova Scotia Health Authority. The purpose of this performance audit was to determine whether there is appropriate IT governance in place for the health care sector.

It is our role to independently express a conclusion about whether the Departments of Health and Wellness and Internal Services, IWK Health Centre, and Nova Scotia Health Authority comply in all significant respects with the applicable criteria. Management at the Departments of Health and Wellness and Internal Services, IWK Health Centre, and Nova Scotia Health Authority acknowledged their responsibility for IT governance in the health care sector.

This audit was performed to a reasonable level of assurance in accordance with the Canadian Standard for Assurance Engagements (CSAE) 3001 – Direct Engagements set out by the Chartered Professional Accountants of Canada; and Sections 18 and 21 of the Auditor General Act.

We applied the Canadian Standard on Quality Control 1 and, accordingly, maintained a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

In conducting the audit work, we complied with the independence and other ethical requirements of the Code of Professional Conduct of Chartered Professional Accountants of Nova Scotia, as well as those outlined in Nova Scotia's Code of Conduct for public servants.

The objectives and criteria used in the audit are below:

Objective:

To determine whether the Health Authority, IWK, and the Departments of Internal Services and Health and Wellness have appropriate IT governance in place for the health care sector.

Criteria:

1. The selected entities should establish an IT governance framework to provide accountability and oversight.
2. The selected entities should have implemented IT risk management frameworks.
3. The selected entities should have processes in place to align IT with the needs of the business.
4. The selected entities should ensure agreed-upon service levels have been met.
5. The selected entities should monitor controls to ensure they are designed and operating effectively.
6. The selected entities should evaluate and assess independent assurance reports.



Criteria for the audit are from the IT Governance Institute's framework, COBIT 4.1, which is generally accepted as an international authoritative source of best practices for the governance, control, management, and audit of IT operations. The criteria were accepted as appropriate by senior management at the entities audited.

Our audit approach consisted of interviewing management and other key personnel and reviewing documentation to determine whether management and those charged with oversight responsibilities established an IT governance framework; considered the Province's health care goals in IT strategies; implemented processes to determine, evaluate, and manage IT risks; and monitored key IT controls, service level agreements, and independent assurance reports. Our audit covered the period April 1, 2015 to March 31, 2018. We examined documentation outside of that period as necessary.

We obtained sufficient and appropriate audit evidence on which to base our conclusion on November 14, 2018, in Halifax, Nova Scotia.

Based on the reasonable assurance procedures performed and evidence obtained, we have formed the following conclusions:

- The Department of Health and Wellness is not providing effective leadership and direction on IT in the health sector.
- The Departments of Health and Wellness and Internal Services, IWK Health Centre, and Nova Scotia Health Authority do not have not formalized roles and responsibilities for IT in the health care sector and are not adequately managing IT risks.